Fiche-conseils

CHOISIR SON MOT DE PASSE AVEC SOIN

Un des éléments de base de la sécurité informatique, le mot de passe est le moyen d'authentification le plus utilisé. Combiné avec un nom d'utilisateur, il permet de s'identifier et d'accéder à sa messagerie, à son compte informatique ou bien encore à toutes sortes de services et ressources en ligne bénéficiant d'un accès protégé et sécurisé. Plus largement, il joue un rôle primordial dans l'accès aux messages, documents et données personnelles. Pour préserver la sécurité et la confidentialité de ses données personnelles, choisir de bons mots de passe est indispensable.

Définition d'un bon mot de passe

Difficile tant à deviner par une personne tierce qu'à trouver à l'aide d'outils automatisés tout en restant facile à retenir, un bon mot de passe se caractérise par :

- une combinaison inhabituelle de lettres, chiffres et symboles ;
- un minimum de 10 caractères, idéalement 12 à 16 caractères ;
- une absence de signification précise.

À proscrire

- Suites logiques (azerty, qwertz, asdfgh, abcdefg, aaaaaa, 1234567...)
- Mots connus ou références existantes, quelle que soit la langue (mots du dictionnaire, noms propres, lieux...)
- Tout ou partie de mots en rapport avec des informations personnelles (nom, prénom, date de naissance, matricule, n° téléphone, n° d'immatriculation...)
- Les 'traditionnels' mots de passe considérés comme faible (sesame, password, motdepasse...)

Conseils pour créer un bon mot de passe

1. Choisissez une phrase ou un vers facile à retenir.
2. Conservez les initiales de chaque mot de la phrase ou du vers choisit.
3. Remplacez certaines lettres par des chiffres ou symboles ou rajoutez un chiffre supplémentaire.

Exemple 1	Exemple 2
Faire son jogging c'est agréable et bon pour la santé !	Brrrr, il fait vraiment froid ce matin, -9 degrés !
↓	↓
Fsjcaebpls!	Bifvfcm-9d!
↓	↓
Fsjcabpls!52	B,ifvfcm-9d!

Recommandations et responsabilité

Vous êtes responsable de votre compte informatique, et devez en assurer sa sécurité. Si un pirate parvient à trouver votre mot de passe, il pourra non seulement accéder à votre messagerie électronique et votre compte informatique, mais également utiliser le compte usurpé pour envoyer du spam ou des e-mails d'hameçonnage, exploitant ainsi les ressources disponibles à toute fin qu'il jugera utile (avec des implications et conséquences pour vous-même, mais aussi pour d'autres utilisateurs).

Choisissez des mots de passe uniques

N'utilisez pas le même mot de passe pour tous vos comptes et accès, car en cas de vol, la personne qui l'aura subtilisée aura accès… à tout.

Gardez vos mots de passe secret

Ne le donnez à personne, sous aucun prétexte et, surtout, ne le transmettez jamais par e-mail, messagerie directe ou téléphone, même si on vous le demande !

Protégez vos mots de passe

Ne les inscrivez pas en clair dans des documents ou sur des morceaux de papier facilement accessibles.

restena
réseau · sécurité · .lu

Principales attaques sur les mots de passe

Attaque par force brute (par recherche exhaustive)

Méthode technique destinée à générer exhaustivement toutes les combinaisons de caractères possibles.

Plus votre mot de passe est varié dans le type de caractères, plus il résistera aux attaques.

Attaque par dictionnaire

Méthode technique consistant à tester une série de mots issus d'un dictionnaire (noms, prénoms, mots de passe communs, films, villes, etc.), souvent utilisée en complément de l'attaque par force brute.

Pour augmenter les chances de trouver (casser) un mot de passe, les logiciels automatisés appliquent des transformations aux mots telles que :

- le changement de la casse de certaines lettres (exemple : aViOn) ;
- l'ajout d'un chiffre ou symbole au début ou à la fin d'un mot (exemple : 9marc, maison!) ;
- le remplacement de certains caractères par des chiffres ou des symboles (exemple : mai5on, mai!on).

Des mots de passe tels que 'aVion12' ou 'marc123' auront de grandes chances d'être trouvés.

→ Changez votre mot de passe dès que vous avez le moindre doute sur son caractère personnel et confidentiel.

Attaque par ingénierie sociale / hameçonnage / *phishing*

Méthode amenant les internautes à révéler des informations personnelles ou sensibles (mot de passe, code PIN, informations bancaires) via un message électronique ou un site web frauduleux.

Escroquerie très répandue sur Internet, le *phishing* (hameçonnage ou filoutage) repose sur l'ingénierie sociale et exploite la « faille humaine », la confiance, la crédulité ou l'ignorance de l'internaute.

Restez vigilant !

- Ne divulguez jamais vos informations confidentielles que ce soit via e-mail, téléphone ou tout autre manière suspecte.
- Ne saisissez aucune information personnelle dans des formulaires reçus par courrier électronique.

Attaque par enregistreur de frappe (*keylogger*)

Méthode visant à récupérer les mots de passe et autres données sensibles directement sur le clavier, en clair.

Programme espion (*spyware*) tournant sur l'ordinateur à l'insu de l'utilisateur, l'enregistreur de frappe (*keylogger*) enregistre toutes les entrées clavier et envoie les données collectées aux réseaux des pirates.

Restez vigilant !

- Installez uniquement sur votre ordinateur des logiciels dont vous connaissez l'origine.
- Installez et gardez à jour vos logiciels anti-virus / anti-*spyware* ainsi que le pare-feu (*firewall*) pour protéger votre ordinateur contre les virus, chevaux de Troie et programmes espions.
- Soyez extrêmement prudent lorsque vous vous connectez sur un ordinateur qui n'est pas sous votre contrôle (cybercafé, hôtel, etc.) : vous ne savez pas quels types de logiciels y sont installés ni s'il y a des programmes espion sur la machine.

Offre de services

Pour bénéficier pleinement des services proposés par la Fondation Restena, un mot de passe est requis. Vous pouvez à tout moment le changer en vous connectant à l'outil de « Gestion de compte en ligne » sous account.restena.lu

Important : La Fondation Restena ne vous demandera jamais votre mot de passe ni par téléphone, ni par courrier électronique !

restena
réseau · sécurité · .lu